REMARKS/ARGUMENTS

Reconsideration of the rejection of claims 26-33 and 42 under 35 USC §103(a) is respectfully requested on the grounds that the reference on which the rejection is based, U.S. Patent No. 2002/0124178 (the Kocher publication), filed on **September 5, 2002**, is **not prior art** with respect to the present application, which has an effective filing date of **May 18, 1998** (the filing date of the parent PCT application). The Kocher publication has one parent application with a filing date of January 2, 1998 (provisional appl. **Ser. No. 60/070,344**), but this application **does not include the teachings relied upon for the rejection**. The argument that Kocher is not prior art was not included in the Appeal Brief or Reply Brief was first presented in a Request for Rehearing, but the Board determined that it was a new argument and refused consideration. Accordingly, it is being presented with a Request for Continued Examination.

The Kocher publication is relied upon by the Examiner for its disclosure of performing blinding operations using auxiliary data, as explained in item 6 on page 14 of the final Office Action dated January 20, 2011:

> a method of protecting secret data stored in a semiconductor chip of a data carrier, where the method includes **falsifying input data by combination with auxiliary data before execution of one or more operations and executing those operations on the semiconductor chip** (paragraphs 0068, 0070, and 0072, where blinding occurs before permutation operations), and **combining the output data with an auxiliary function value in order to compensate for the falsification of the input data** (paragraphs 0070, 0072, and 0073, where unblinding occurs to compensate for the blinding), **where the auxiliary value was determined by executing the operations using the auxiliary data as input data** (paragraph 0072, where the output buffer is initialized with the blinding bit and the data in the output buffer is the result of using the input permutation table, i.e., the operations).

However, the teachings concerning falsifying input data by combination with auxiliary data and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data, which are included in the Kocher publication filed on December 3, 2001,

- **are *not* included in provisional application Ser . No. 60/070,344, filed January 2, 1998, on which priority of the Kocher publication is based.**

Since the present application is based on a PCT application filed on **May 18, 1998**, the Kocher publication is not prior art against the present application unless the priority application filed on January 2, 1998, contains the teachings relied upon for the rejection. The only one of the priority applications that has a filing date earlier than May 18, 1998, is provisional application Ser. No. 60/070,344 (hereinafter, "the Kocher provisional").

While the Kocher publication includes a detailed description of blinding (including an explanation, deemed irrelevant by the Examiner and the Board, concerning the specific manner in which blinding is carried out by generating of auxiliary values during blinding), **the Kocher provisional application** ***does not mention either falsifying input data by combination with auxiliary data or combining the output data with an auxiliary function value in order to compensated for the blinding***. Instead, the Kocher provisional's disclosure of blinding is limited to the following statements, which do not support even the conclusory statement of "collective teachings" on which the rejection was based.:

Page 2, lines 17-21 of the Kocher provisional:

> Some techniques for hindering external monitoring of cryptographic secrets are known, such as using power supplies with large capacitors to mask fluctuations in power consumption, enclosing devices in well-shielded cases to prevent electromagnetic radiation, message blinding to prevent timing attacks, and buffering of inputs/outputs to prevent signals from leaking out on I/O lines. Shielding, introduction of noise, and other such countermeasures are often, however, of limited value, since skilled attackers can still find keys by amplifying signals and filtering out noise by averaging data collected from many operations. Further, in smartcards and other tamper-resistant chips, these countermeasure are often inapplicable or insufficient due to reliance on eternal power sources, impracticality of shielding, and other physical constraints. The use of blinding and constant-time mathematical algorithms to prevent timing attacks is also known, but does not prevent more complex attacks such as power consumption analysis. . .

Page 3, lines 1-6:

> The present invention makes use of previously-known cryptographic primitives and operations. For example: U.S. patent 5,136,646 to Haber et al. And the pseudorandom number generator used in the RSAREF cryptographic library use repeated application of has functions; anonymous digital cash schemes use blinding techniques; zero knowledge protocols use has functions to mask information; and key splitting and threshold schemes store secrets in multiple parts.

Page 19, lines 9-12:

> One way to improve performance is to remove the blinding and unblinding operations, which are often unnecessary. (The blinding operations prevent attackers from correlating input values of y with the numbers processed by the modular exponentiation operations).

These are the only passages in the Kocher provisional that use the term "blinding." There are no passages that correspond to the passages relied upon by the Examiner in the final Office Action, namely paragraphs 0070, 0072, and 0073 of the Kocher publication. Therefore, these relied-upon teachings in the Kocher publication are not supported by the Kocher provisional, and are not prior art with respect to the claims of the present application. Since the Kocher publication is not prior art with respect to the present application, withdrawal of the rejection of claims 26-33 and 42 under 35 USC §103(a) is respectfully requested.

Having thus overcome the sole rejection made in the final Office Action, withdrawal of the rejection and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

/Benjamin E. Urcia/

Date: January 14, 2013

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

S:\Producer\beu\Pending Q...Z\V\VATER 700656\ResponseWithRCE.wpd